Breach

Information Technology Board

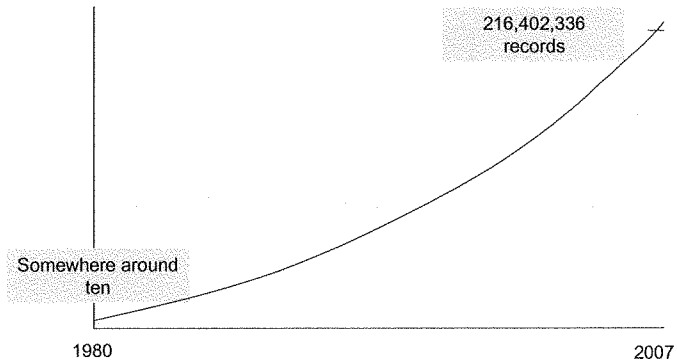
December 5, 2007

Agenda

- Background/Perspective
- Environment/Risks
- What Constitutes a Breach?
- Best Practice
- Montana Statute

Background

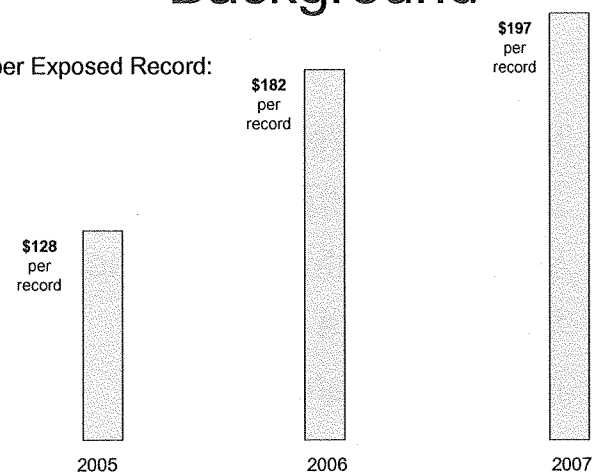
Number of records containing sensitive personal information involved in security breaches in the U.S…



Source: privacyrights.org

Background

Cost per Exposed Record:



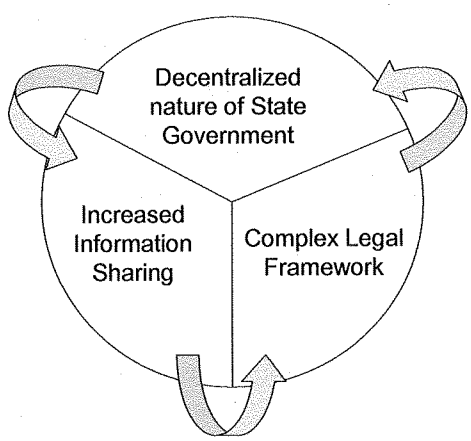
Source: Ponemon Institute

Some Perspective

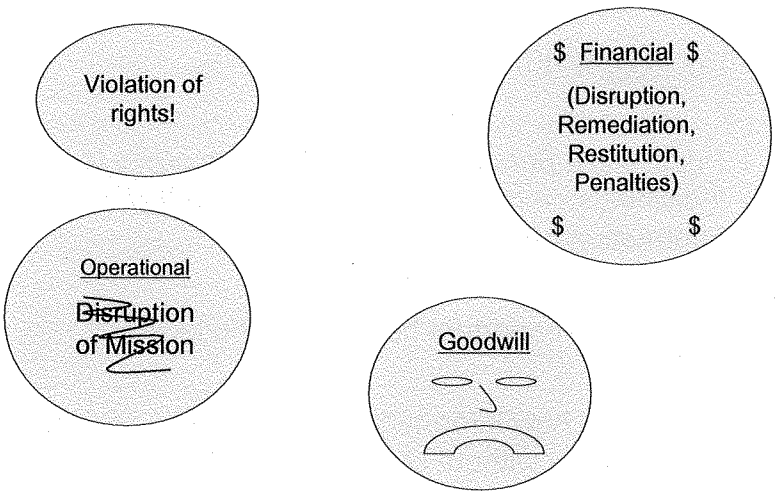
Privacy is a defining issue of the day…

- Privacy is a *personal construct* that accrues to individuals...a person may have a *right* that personal information be secured…
- It becomes important because of the lack of it…
- Security is how information is protected…one cannot have privacy without security

Our Privacy Environment



Risks…



What Constitutes a Breach?

- Time-based
  "It's a breach today, not tomorrow" or…
  "It wasn't yesterday…today it is."
- Legal-based → change in law
- Context-based
  "This is sensitive when combined with that…but not when combined with those."

Best Practice

- Fair Information Principles (FTC) → Your North Star
- Define Information → Information Management Life Cycle
- Protect Information → Security
- Prepare for Breach → "Breach Plan"
- Notification → Execute Plan
- Follow-up → Damage Assessment

Best Practice Notes…

Fair Information Principles (FTC) …

1. Notice/Awareness – of collection and intended use
2. Choice/Consent – provide a choice; means of consent
3. Access/Participation – permitting personal access to own information
4. Integrity/Security – appropriate measures to secure collected information
5. Enforcement/Redress – enforcing policies; providing a means of citizen redress

Constraints

Best Practice Notes…

Define Information…

- Data owner
- Data custodian
- "Notice-triggering" information
- Classify risk
- Classify information

Information Management Life Cycle

Best Practice Notes…

Protect Information…

- Collect minimal amount
- Maintain inventory
- Protect by sensitivity
- Use physical and technology safeguards
- Protect high-risk environments/devices
- Train users
- Enforce policy
- Encryption
- Dispose of records
- Define intrusion
- Review security plan…including Breach Plan

Best Practice Notes…

Prepare for Breach…Breach Plan…

- Adopt written policies and procedures
- Designate roles & responsibility
- Train employees
- Include breach within Incident Response Plan
- Plan measures to contain, control and correct
- Require notification of data owners
- Identify law enforcement contacts
- Consider law enforcement recommendations
- Document response actions
- Review Incident Response Plan annually

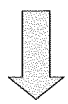
Best Practice Notes…

Notification: Execute Breach Plan… (Incident Response)

- Detection: Acquisition of triggering information
- Timing of notification
- Contact law enforcement
- Whom to notify
- Contact credit reporting agencies
- Content of notice
- Form and style of notice
- Means of notification

Best Practice Notes…

- Follow-up…
  - Certify closure of breach → "Are we secure?"
  - Policy/standards implications → changes?
  - Credit reporting support → fund the monitoring program?
  - Public relations campaign → re-build reputation?



Damage Assessment

Montana Statute

– MCA 30-14-1701, et seq.

…means unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by the person or business and causes or is reasonably believed to cause loss or injury to a Montana resident.

– MCA 2-15-114

…Department heads have overall responsibility for…security for all data

MCA 30-14-1704

- Disclosure law
- Applies to "…any person" conducting business
- Covers…
  - Personal info in owned or licensed computerized data
  - Defines "personal information"
  - Notification methods
- Does not cover…
  - Damages
  - Restitution
  - Cost to implement